

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

CHANGLIN PIAO,

*Defendant.*

**UNDER SEAL**

Case No. 1:25-MJ-340

**AFFIDAVIT IN SUPPORT OF PROBABLE CAUSE**

I, Samantha Wendt, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since June of 2023. I am currently assigned to the Washington Field Office. My primary duties include investigating violations of federal law, including securities fraud, wire fraud, bank fraud, and internet-enabled crimes. Part of those duties include investigating instances of wire fraud and bank fraud being used for financial gain at the expense of others. Before my career as an FBI Special Agent, I was employed as a Forensic Accountant by the FBI in the Seattle Field Office for two years. As part of that role, I conducted the financial portion of investigations, which included reviewing financial records and determining the sources and uses of funds. I have participated in numerous investigations related to financial crimes and have experience analyzing financial documents, interviewing suspects and witnesses, and reviewing evidence obtained from physical and digital search warrants. I am also a Certified Public Accountant and a Certified Fraud Examiner.

2. I make this affidavit in support of criminal complaint and arrest warrant charging that, from in or about April 2023 and continuing through at least February 2024, in the Eastern District of Virginia and elsewhere, defendant **CHANGLIN PIAO** (hereinafter “PIAO”), and others, have committed violations of 18 U.S.C. §1956(h) (Conspiracy to Commit Concealment Money Laundering). In sum, PIAO, with co-conspirators, conspired to execute a multi-million-dollar scheme to launder funds obtained from victims of elder fraud scams.

3. I have personally participated in this investigation and have witnessed many of the facts and circumstances described herein. The information set forth in this affidavit is based on my own personal knowledge, my review of relevant records, reliable information provided to me by other law enforcement officers, and my training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. Unless otherwise indicated, all written and oral statements referred to herein are set forth in substance and in part, rather than verbatim. Where I assert that an event took place on a particular date or at a particular time, I am asserting it took place on or about the date alleged or at that approximate time.

#### PROBABLE CAUSE

##### **I. RELEVANT INDIVIDUALS AND ENTITIES**

4. PIAO is a 36-year-old male and is currently believed to be located in Westmont, Illinois.<sup>1</sup>

---

<sup>1</sup> On May 15, 2025, U.S. Magistrate Judge William B. Porter approved a warrant for the location data associated with PIAO’s cell phone. *See* Case Nos. 1:25-sw 431 and 1:25-ec-985. The data obtained from that warrant confirmed that PIAO is in the Northern Illinois area.

5. Co-Conspirator-1 is a 42-year-old male with an address in Flushing, New York.<sup>2</sup>
6. Co-Conspirator-2 is a 37-year-old male with an address in Las Vegas, Nevada.<sup>3</sup>
7. Co-Conspirator-3 is 43-year-old male with an address in Flushing, New York.
8. Victim-1 is a 74-year-old resident of Connecticut.
9. Company-1 is a shared office space provider headquartered in Beverly,  
Massachusetts.
10. Company-2 is an energy company headquartered in Richmond, Virginia.
11. Company-3 is an apartment leasing company located in Arlington, Virginia.
12. Company-4 is a casino and hotel located in Oxon Hill, Maryland.
13. Individual-1 is a 48-year-old male located in Brooklyn, New York.
14. Individual-2 is a 51-year-old male located in Short Hills, New Jersey.
15. Bank-1 is a financial institution headquartered in Toronto, Canada.
16. Bank-2 is a financial institution headquartered in Pittsburgh, Pennsylvania.
17. Bank-3 is a financial institution headquartered in Charlotte, North Carolina.
18. Bank-4 is a financial institution headquartered in New York, New York.
19. Bank-5 is a financial institution headquartered in San Francisco, California.
20. Bank-6 is a financial institution headquartered in Charleston, West Virginia.
21. Bank-7 is a financial institution headquartered in Charlotte, North Carolina.
22. Bank-8 is a financial institution headquartered in New York, New York

---

<sup>2</sup> On July 25, 2024, a grand jury in this District indicted Co-Conspirator-1 and Co-Conspirator-2 on one count of conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h) and six counts of concealment money laundering, in violation of 18.U.S.C. §§ 1956(a)(1)(B)(i) and 2. *See* Case No. 1:24-cr-170.

On September 6, 2024, Co-Conspirator-1 pled guilty to one count of conspiracy to commit money laundering.

<sup>3</sup> On November 1, 2024, Co-Conspirator-2 pled guilty to one count of conspiracy to commit money laundering.

## **II. THE SCHEME TO DEFRAUD**

23. The FBI, the Treasury Inspector General for Tax Administration (“TIGTA”), and the United States Postal Inspection Service (“USPIS”) (collectively, the “Joint Investigation”), are investigating a conspiracy which exploits the Internal Revenue Service’s (“IRS”) Modernized Internet Employer Identification Number (“Mod IEIN”) online portal. Mod IEIN is the IRS system that allows users to register for a unique Employer Identification Number (“EIN”) for a business. These transactions are processed at IRS Enterprise Computing Centers located in West Virginia and Tennessee, making each of these transactions an interstate wire communication.

24. The investigation shows that PIAO, Co-Conspirator-1, Co-Conspirator-2, and others, obtained EINs for various fictitious businesses in furtherance of a scheme to defraud. These EINs allowed the co-conspirators to open business bank accounts at various financial institutions (including financial institutions in the Eastern District of Virginia) for the purpose of receiving numerous fraudulent wire transfers. Through victim interviews, police reports, the review of complaints submitted to Internet Crime Complaint Center (“IC3”), and the review of information received by victim surveys, law enforcement has determined that many of these wire transfers were the result of a tech support scams targeting elderly individuals. The proceeds of these fraudulently obtained funds were rapidly withdrawn or moved between bank accounts controlled by different co-conspirators. This rapid movement of funds is indicative of communication and coordination between various individuals in furtherance of the conspiracy.

25. The investigation revealed a conspiracy that targeted unsuspecting victims through nationwide elder fraud scams, including tech support scams, government impersonation scams, romance scams, and investment fraud scams. Typically, the victims reported falling victim to a tech support scam. In these instances, victims reported receiving a pop-up on their computer. The pop-ups included a phone number to contact for assistance. Once the victims called the phone

number, the victim was advised to provide the purported technical support individual access to their computer. Upon doing so, the victim was often informed that their bank account had been hacked and the victim needed to secure their financial assets by transferring their money to the bank accounts associated with the conspiracy. The victim—believing they were sending money to address real issues with their computer and bank accounts—either wired money to bank accounts controlled by PIAO, Co-Conspirator-1 and additional co-conspirators or mailed checks to addresses associated with PIAO, Co-Conspirator-1, and additional co-conspirators to be deposited into bank accounts controlled by PIAO, Co-Conspirator-1 and additional co-conspirators.

### **III. THE FICTITIOUS VIRGINIA BUSINESS ENTITIES**

26. On June 16, 2023, Dragon Auto Parts Inc. was incorporated by the Commonwealth of Virginia State Corporation Commission (“SCC”) with a registered agent of Individual-1 and registered office address in Annandale, Virginia. The Annandale, Virginia address is associated with Company-1, which is a company that rents office space to individuals and businesses. The investigation revealed that Company-1 had no records involving Individual-1 or Dragon Auto Parts Inc. renting office space.

27. On June 21, 2023, a Bank-1 account number ending in -6540, in the name of Dragon Auto Parts Inc. (“Dragon Auto Parts Bank-1 account”) was opened at a location in the Eastern District of Virginia. Included in the Bank-1 account opening documents was a Company-2 customer energy bill for Individual-1 showing an address in Arlington, Virginia dated June 5, 2023. Records from Company-2 indicated that they were unable to locate an account associated with Individual-1, the Arlington, Virginia address, or the meter number provided in the Company-2 customer energy bill. Additionally, the Arlington, Virginia address is associated with

an apartment building leased by Company-3. Company-3 had no records involving Individual-1 or Dragon Auto Parts Inc. renting the specified unit number in 2023.

28. I reviewed bank surveillance footage associated with Dragon Auto Parts Bank-1 account. I identified Co-Conspirator-1 in the bank surveillance footage opening the account and conducting financial transactions associated with the account.

29. Between June 26, 2023 and July 13, 2023, the Dragon Auto Parts Bank-1 account was the beneficiary of two wire transfers and one cashier's check deposit totaling over \$139,000. These deposits included a \$39,221.01 wire transfer from Victim-1. On March 4, 2024, I interviewed Victim-1 who verified that the wire transfer to the Dragon Auto Parts Bank-1 account was the result of a tech support scam.

30. Further investigation revealed that business bank accounts were opened for Dragon Auto Parts Inc. (using Individual-1's identity) at other financial institutions, including at Bank-2, Bank-3, Bank-4, Bank-5, and Bank-6. Account opening documents associated with the Bank-5 account in the name of Dragon Auto Parts Inc. indicated the business had five employees and was described as "Tire Shop and Automotive Parts." Financial analysis revealed no deposits or withdrawals consistent with an automotive business.

31. Between June 26, 2023 and October 17, 2023, the bank accounts described above, all opened in the name of Dragon Auto Parts Inc., were the beneficiary of 19 wire transfers and one cashier's check deposit, totaling over \$670,000, all from known or suspected victims. The FBI interviewed nine additional victims that deposited money into the Dragon Auto bank accounts, all indicating that money transfers were the result of a tech support scam.

32. Based on the fraudulent activity described above, I reviewed the Commonwealth of Virginia SCC records to identify additional businesses located at the Annandale, Virginia address associated with Company-1. This review identified several fictitious businesses, including:

- a. M&M Popular Package Food Inc. (registered agent Individual-2)
- b. LL Wang Food Trading Inc. (registered agent L.W.)
- c. CrysAl Accessories Inc. (registered agent H.C.)
- d. Roger Trucking Service (registered agent X.Z.)

33. The investigation has identified each of the businesses referenced above was also associated with the residential address in Arlington, Virginia. Company-1 and Company-3 had no records of the above individuals or entities being associated with their properties.

34. On April 25, 2024, I interviewed Individual-2, whose information was used to incorporate M&M Popular Package Food Inc. Individual-2 indicated that his identity appeared to have been stolen in the summer of 2023. Individual-2 filed a police report on July 10, 2023 related to the identity theft. I have compared the photographs of the individual depicted in the M&M Popular Package Food Inc. bank surveillance footage to the individual I interviewed in April 2024 and do not believe the person depicted in the surveillance footage is Individual-2. I have compared the surveillance footage to known pictures of Co-Conspirator-1. Based on my review, I believe the person depicted in the surveillance footage (purporting to be Individual-2) to be Co-Conspirator-1.

35. Upon reviewing various bank records, IRS's Mod IEIN records, Postal Service Records and the Virginia SCC records, numerous businesses have been identified as being operated by PIAO, Co-Conspirator-1, and/or other co-conspirators in furtherance of the scheme.

The businesses identified include, but are not limited to, the following (collectively the “Fictitious Virginia Business Entities”):

- a. Dragon Auto Parts Inc
- b. M&M Popular Package Food Inc
- c. LL Wang Food Trading Inc
- d. Crystal Accessories Inc
- e. V&L Good Food Wholesale Inc
- f. Dug Duy Food Trading Inc
- g. Coco Love Nail Art Wholesale Inc
- h. Kim Fashionable Clothing Inc
- i. Leslie Cell Phone Accessories
- j. Roger Trucking Service
- k. Above and Beyond Heating Corp
- l. Kunblo Spring City Inc
- m. SZ Façade Management Inc
- n. Universe CCK Computer Inc
- o. Dragon Façade Management
- p. Hong & Yun Clothing Inc
- q. LMH Computer Service Inc
- r. Carson Truck Service Inc
- s. Phenix Beauty Supplies Inc
- t. Chia Supplies Co Limited
- u. Lena Castle Inc



- v. S&W Façade Management Inc
- w. Pure Life HL Inc
- x. BHB Products Trading Inc
- y. LT Restaurant Supplies Inc
- z. SSW Investment Inc
- aa. UJS Equipment Inc
- bb. Amcor Plus One Wholesale Inc

#### **IV. THE BANK ACCOUNTS OPENED IN THE NAME OF THE FICTITIOUS BUSINESSES**

36. To date, I have reviewed over 100 bank accounts associated with the Fictitious Virginia Business Entities. Review of the bank account activity associated with the Fictitious Virginia Business Entities did not identify transactions that appeared to be legitimate business income or expenses. Rather, the bank accounts have nearly no activity other than the receipt of victim funds and the transfer of those funds to other bank accounts or the cash withdrawal of funds.

37. The bank accounts were often only kept open for a couple of months before being closed by the banks. Accordingly, each Fictitious Virginia Business Entity often held bank accounts at multiple financial institutions. For example, bank accounts associated with Dragon Auto Parts were opened at seven different banks. All seven of the Dragon Auto Parts bank accounts were opened between June 21, 2023 and September 5, 2023 and all the accounts had been closed by November 2023.

38. In total, based on the records I have reviewed, I have probable cause to believe that the Fictitious Virginia Business Entities received over \$12 million in victim funds. I have participated in interviews with over 20 victims who sent over \$1 million to the Fictitious Virginia Business Entities associated with elder fraud scams. In total, I have conducted interviews or

reviewed police reports, IC3 complaints, and victim surveys covering over \$5.5 million in deposits to the Fictitious Virginia Business Entities. The remaining deposits into the Fictitious Virginia Business Entity bank accounts were indicative of being elder fraud proceeds because they appeared to be sourced from elderly individuals located across the United States.

39. Funds from the Fictitious Virginia Business Entity bank accounts were then withdrawn, transferred between bank accounts, and/or wired to bank accounts linked to other suspected fictitious businesses. Based on my training and experience, I submit there is probable cause to believe: (1) that these transactions were conducted to conceal the illicit source of these funds, and (2) that the co-conspirators used or attempted to use the fictitious business bank accounts to launder the proceeds of this fraud scheme.

40. Based on my review of bank surveillance footage, an individual resembling Co-Conspirator-1 was depicted conducting financial transactions associated with at least eight different entities, including Dragon Auto Parts Inc, LL Wang Food Trading Inc, Kunblo Spring City Inc, Crystal Accessories, M&M Popular Package Food Inc, SZ Façade Management Inc, Roger Trucking Service Inc, and Kim Fashionable Clothing Inc. I also observed an individual resembling Co-Conspirator-3 depicted conducting an ATM cash withdrawal from a Dragon Auto Parts account and an individual resembling PIAO conducting transactions associated with the Roger Trucking Service bank accounts. During a September 6, 2024 interview with Co-Conspirator-1, Co-Conspirator-1 corroborated that the individuals depicted in the bank surveillance reviewed were Co-Conspirator-3 and PIAO. None of the bank account signature cards indicate that Co-Conspirator-1, Co-Conspirator-3, or PIAO are authorized signors. The bank account signatories associated with each of the Fictitious Virginia Business Entities are different.

41. In addition to the wire withdrawals, over \$1 million in cash withdrawals appeared to be conducted from the Fictitious Virginia Business Entity bank accounts. The Fictitious Virginia Business Entity bank accounts were also utilized to fund travel expenses (*e.g.*, flights, gas, hotels), luxury goods purchases, Zelle payments, lease payments and food purchases. Some of the transactions conducted included the following:

- a. I obtained records from Company-4 related to PIAO, Co-Conspirator-1, and Co-Conspirator-3. In part, those records indicated that payments from at least four Fictitious Virginia Business Entities – M&M Popular Package Food Inc, Ayang Marketing, YL Restaurant Supplies Inc, 2R Supplies – benefited PIAO's Company-4 account. The records also indicated that Co-Conspirator-3's Company 4 account benefited from a payment from M&M Popular Package Food Inc.
- b. In 2024, over \$195,000 in cashier's checks were made payable to Changlin Trading Inc from two of the Fictitious Virginia Business Entities. Changlin Trading Inc was a business entity associated with PIAO and registered in New York in January 2023.
- c. Between February 29, 2024 and March 18, 2024, a Bank-3 account in the name of 2R Supplies made payments to Securus Inmate, a phone system associated with incarcerated individuals. I reviewed jail call records when Co-Conspirator-1 was detained and noted that the payments from the Bank-3 account in the name of 2R Supplies corresponded to information shared in Co-Conspirator-1's jail calls with a phone number ending in 7156. I believe this phone number is

utilized by PIAO, in part, because it was associated with PIAO's Company-4 account.

42. The above transactions are significant because they further indicate that PIAO was associated with numerous of the Fictitious Virginia Business Entities and benefited from the fraud scheme.

**V. WECHAT CONVERSATIONS FURTHER CONNECT PIAO TO THE CRIMINAL SCHEME**

43. On April 30, 2024, a federal search warrant (1-24-SW-304) was issued by U.S. Magistrate Judge Ivan D. Davis in the Eastern District of Virginia for three devices obtained from Co-Conspirator-1's hotel room. On the cell phone associated with a phone number connected to Co-Conspirator-1, I reviewed WeChat communications between Co-Conspirator-1 and others, including PIAO and Co-Conspirator-3.<sup>4</sup> The WeChat communications included identification documents, Virginia SCC incorporation documents, utility bills, and financial information associated with many of the Fictitious Virginia Business Entities.

44. I reviewed a WeChat group chat called "RW" which included a WeChat account associated with Co-Conspirator-1, a WeChat account with the username "Breaking Waves" and WeChat ID wxid\_\*\*\*\*\*4a12, a WeChat account with the username "Limonade" and WeChat ID a\*\*\*\*8569, a WeChat account with the username "Guan Guan" and WeChat ID xid\_\*\*\*\*\*2212, and a WeChat account with the username "Boss Xie" and WeChat ID wxid\_\*\*\*\*\*6j22.

45. The RW WeChat conversation was almost exclusively used to discuss the fraud scheme. Namely, the conversation covered when to expect victim deposits into the Fictitious

---

<sup>4</sup> These communications primarily occurred in Mandarin and have been translated into English. The information described below is based on my review of those English translations.

Virginia Business Entity accounts, which Fictitious Virginia Business Entity accounts to direct victim funds be deposited into, and where to send the victim funds once received. Review of the RW WeChat conversation also revealed the exchange of bank account information, such as passwords and account numbers, associated with many of the Fictitious Virginia Business Entities and bank accounts linked to other suspected fictitious businesses. I believe this was done to enable multiple people to have access to the bank accounts in order to conduct and review financial transactions.

46. I submit there is probable cause to believe that the Breaking Waves and Limonade WeChat accounts are controlled by PIAO, in part, for the following reasons:

- a. On October 28, 2023, the Breaking Waves WeChat account sent a direct message to Co-Conspirator-1 with a photograph of a Company-4 rewards card in the name of PIAO.
- b. On December 19, 2023, the Breaking Waves WeChat account sent a direct message to Co-Conspirator-1 with a photograph of a Virginia SCC webpage directing the individual to upload Articles of Incorporation. The image depicts the message “Hi, Changlin Piao.” I reviewed bank account opening documents from TD Bank associated with Chia Supplies Co Limited, one of the Fictitious Virginia Business Entities, and noted a December 19, 2023 receipt from the Virginia SCC related to the registration of Chia Supplies Co Limited. The receipt was addressed to PIAO and included his New York address.
- c. On December 28, 2023, the Boss Xie WeChat account tagged the Limonade WeChat account in a message and asked: “Boss Pu, send another account to receive chat scam money.” I noted multiple instances of PIAO being referred to

as Xiao Pu in the RW Group Chat and both the Limonade and Breaking Waves WeChat accounts responding. Based on my training and experience, I am aware that when the word Xiao is placed before a name it is often used to show familiarity with someone or to express that the person is younger or has an inferior status to the speaker. Xiao is commonly interpreted to mean “little.”

- d. On December 28, 2023, the Boss Xie WeChat account tagged the Limonade WeChat account in a message and asked “Bro, can this receive code?” Approximately 30 minutes later, with no additional discussion in the group chat, the Breaking Waves WeChat account responded “Wait, I just came out, sorry.” This indicates that PIAO utilized the Limonade and Breaking Waves WeChat accounts interchangeably.
- e. In a September 6, 2024 interview, Co-Conspirator-1 stated that the Breaking Waves and Limonade WeChat accounts were both controlled by PIAO

47. Accordingly, hereinafter, references to the Breaking Waves and Limonade WeChat accounts will be referred to as PIAO.

48. I also reviewed a direct WeChat conversation between Co-Conspirator-1 and PIAO (via the Breaking Waves WeChat account). The conversation revealed that they would exchange numerous credit reports, driver’s license photographs, social security numbers, addresses, and dates of birth for the individuals listed as registered agents and signatories for the Fictitious Virginia Business Entities.

49. On November 16, 2023, Guan Guan asked for the preparation of “the specialized account just for receiving the scam chat, and then get a few corporate entities to receive the

cashier's checks." Guan Guan further stated: "the customer is pushing me daily to send accounts."

A few hours later, PIAO responded with the following account information:

*CITI BANK TOKEN*

*Business name BHB PRODUCTS TRADING INC*

*Business code 7000000000645147*

*User id 463*

*Password Cal210038@*

*Business Checking*

- *Name: BHB PRODUCTS TRADING INC*

- *Address of company 6801 Richmond HWY STE 201 Alexandria VA 22306*

- *Account#: 9250977018*

- *Fedwire ABA for wires: 254070116*

*Address of bank : 3241 14th st nw Washington DC 20010*

*ONLINE BANK hb1980bao*

*PASSWORD : Cal210038@*

50. BHB Products Trading Inc is one of the Fictitious Virginia Business Entities. I reviewed BHB Products Trading Inc bank accounts held at Bank-1, Bank-3, and Bank-4. These accounts appeared to receive over \$700,000 in victim funds.

51. Review of the WeChat conversations further indicated that PIAO, Co-Conspirator-1, Guan Guan and other co-conspirators, accessed and attempted to access the bank accounts using the account information provided. For example, on January 11, 2024, Guan Guan stated: "I received several transactions for this one at [Bank-8]," and "[c]heck the verification code." Less than one minute later, PIAO responded with a picture of a cell phone receiving a text message from Bank-8 with a two-factor authentication code. I believe that PIAO provided this information to Guan Guan so that Guan Guan could review bank account activity associated with one of the Fictitious Virginia Business Entities.

52. Review of the bank account opening documents indicated that a Company-2 utility bill associated with account number ending -8664, meter number ending -5442, was often submitted

for address verification. Records from Company-2 indicated that the meter number did not exist and that the account number was associated with an unrelated government entity. In reviewing the WeChat conversations, I identified numerous instances in which fictitious Company-2 utility bills were shared for different entity names, registered agent names, and addresses. Notably, on January 21, 2024, Guan Guan informed PIAO, Co-Conspirator-1 and co-conspirators that they were trying to create a new cryptocurrency account and they needed to provide proof of address in Virginia. PIAO responded: "All are fake." PIAO also provided the following image, depicting the areas of the utility bill that needed to be changed:

53. The signatory cards associated with the account opening documents for the Fictitious Virginia Business Entities often indicated fictitious business purposes for the accounts. At times, incoming wire memos from victims reference fictitious business purposes, such as the purchase of a home, goods, or to support a friend's new business. Conspirators would often tell victims



what to put in the wire memo line when sending the wire. For example, a Bank-4 account in the name of Ayang Marketing was opened in October 2023 and listed the business description as “[s]elling smart phone and iPad accessories wholesale.” On November 14, 2023, in reference to Ayang Marketing, Guan Guan asked “[w]hat’s the business scope for this company?” because “[t]he payment note is required. to put down what was bought.” PIAO responded “cellphone & computer accessories wholesale.” Ayang Marketing is one of the Fictitious Virginia Business Entities. I reviewed Ayang Marketing bank accounts held at Bank-1, Bank-3, Bank-4, and Bank-7. These accounts received over \$450,000 in victim funds and, as discussed above, also benefited PIAO’s Company-4 account.

54. As discussed in the WeChat conversations, the true source of the funds for the Fictitious Virginia Business Entities derived from tech support and other elder fraud scams. On December 11, 2023, the following conversation occurred in the RW Group Chat:

*Guan Guan: Two deposits have been arranged: one for fifty thousand and the other for sixty thousand.*

*Guan Guan: One more account*

*Guan Guan: to receive money from the scam chats.*

*PIAO: Currently there isn’t any*

*Guan Guan: Here comes one from the [Bank-4].*

*PIAO: scam chat?*

*Guan Guan: yes*

55. Review of the RW Group Chat also included instructions on where to send the funds deposited into the bank accounts associated with the Fictitious Virginia Business Entities. For example, on December 7, 2023 Guan Guan provided the bank account information for Luou

Trading Co Limited and stated “account for return funds.” PIAO responded by providing a copy of an outgoing wire receipt in the amount of \$37,699 to Luou Trading Co Limited from a BHB Products Trading Inc account held at Bank-4. Guan Guan provided numerous accounts as withdrawal accounts for the scam proceeds, including: AUS Merchant Services, Kelsea Limited, and Tiger Fly Co. Notably, records from Bank-8 indicated that even though the outgoing wires to Bank-4 accounts associated with Tiger Fly Co and Kelsea Limited appear to be credited to U.S.-based financial institutions, the true beneficiary is AUS Merchant Services, which is associated with Alipay. Based on my training and experience, I believe that these outgoing wires are a method to move the victim funds from the United States back to China.

\* \* \*

CONCLUSION

56. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that PIAO has committed violations of 18 U.S.C. §1956(h) (Conspiracy to Commit Concealment Money Laundering). Accordingly, I respectfully request that a criminal complaint be issued charging PIAO with violations of 18 U.S.C. §1956(h) (Conspiracy to Commit Money Laundering). In addition, I respectfully request that a warrant be issued for the arrest of the PIAO.

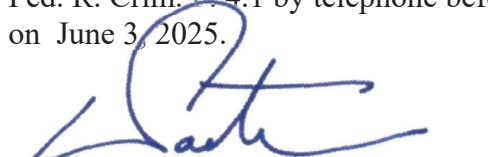
Respectfully submitted,

SAMANTHA  
WENDT

Digitally signed by  
SAMANTHA WENDT  
Date: 2025.06.02 16:27:06  
-04'00'

Special Agent Samantha Wendt  
Federal Bureau of Investigation

Sworn and subscribed to, in accordance with  
Fed. R. Crim. P. 4.1 by telephone before me  
on June 3, 2025.



Hon. William B. Porter  
United States Magistrate Judge